UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,119	12/22/2003	W. Carey Bunn	END920030045US1	7503

26502 7590 02/02/2011

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
SCHMIDT, KARL	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
02/02/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/743,119	BUNN ET AL.	
	Examiner	Art Unit	
	KARI L. SCHMIDT	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the Board of Appeals Decision filed on 09/09/2010. The examiner notes the instant application is being re-opened after the board decision in light of new grounds of rejection being made for the pending claims. Claims 1-20 are pending in the application

Response to Arguments

Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the examiner notes the Specification does not provide antecedent basis for the claim terminology as recited in claim 16 and 17: "a computer usable medium." The examiner notes that one of ordinary skill in the art needs to utilize the specification in order to determine and interpret what "a computer usable medium" can be? The examiner notes a reasonable interpretation of the "a computer usable medium" can be a medium that can include a signal, thus causing the claim to be non-statutory.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 16 and 17 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, with the specification not defining "a computer program product" makes the claim as a whole be drawn to a software per and "a computer usable medium" (see Specification Objection) can be viewed as a signal which doesn't fall within one of the four statutory categories of invention. Therefore a computer usable medium can be viewed as a signal or carrier wave. Further the examiner notes the claim may be amended by changing "a computer usable medium" to **"non-transitory computer readable medium"** thus excluding that portion of the scope covering transitory signals. The scope of the disclosure given the state-of-the-art covers both transitory and non-transitory media and this amendment would limit the claim to an eligible (non-transitory) embodiment.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 4-10, 16, 18-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Kurtz et al. (US 2003/0217039 A1).

Claims 1, 16, and 18-19

Kurtz discloses a method for checking network perimeter security (see at least, abstract: the examiner notes "a... method provide comprehensive and highly automated testing of vulnerabilities to intrusion on a target network, including identification of operating system, identification of target network topology and target computers, identification of open target ports, assessment of vulnerabilities on target ports, active assessment of vulnerabilities based on information acquired from target computers, quantitative assessment of target network security and vulnerability, and hierarchical graphical representation of the target network, target computers, and vulnerabilities in a test report"), said method comprising the steps of: reviewing security of a network perimeter architecture (see at least, [0012]: the examiner notes the "network typically includes one or more computers, where a computer includes a desktop station running any operating system, a router, a server, and/or any other networked device capable of sending and

receiving packets through standard internet protocols" is interpreted to be a network perimeter architecture based on the BPAI Decision rendered on 9/9/2010 stating "a securing assessment is performed for all notes within network architecture, including servers clients, peripheral devices and entries and exists from the network"; further [0012]: the target computers comprise all or a portion of the computers found within the target network and [0019]: the examiner notes "parallel testing of multiple target computers on the network" to be interpreted as reviewing security of a network perimeter); reviewing security of data processing devices that transfer data across the perimeter of the network (see at least, [0012]: the examiner notes "the network typically includes one or more computers, where a computer includes a desktop station running any operating system, a router, a server, and/or any other networked device capable of sending and receiving packets through standard internet protocols" to be interpreted as data processing devices transferring data across the perimeter of the network and [0019]); reviewing security of applications that transfer data across said perimeter (see at least, [0088]: the examiner notes vulnerability assessment routing checks identified operating system is interpreted to be reviewing security of applications that transfer data across said perimeter); reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, [0088]: the examiner notes vulnerability assessment routing checks identified operating system and open ports of a computer); and generating a report concerning security of said perimeter based upon all of the reviewing steps (see at least, abstract).

Claim 4

Kurtz discloses wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of a web server, an e-mail server or an FTP server (see at least, [0012]: the examiner notes a server (e.g. web)).

Claim 5

Kurtz discloses further comprising the step of reviewing security of a server within said perimeter that provides data to said data processing devices that transfer data across the perimeter of said network (see at least, abstract, [0012], and [0019]).

Claim 6

Kurtz discloses wherein each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network (see at least, [0005]: the examiner notes a network administrator would be interpreted to be an enterprise which owns or controls a network and [0449]: the examiner notes acceptable policy).

Claim 7

Kurtz discloses further comprising the step of determining said network perimeter (see at least, abstract and [0012])

Claim 8 and 9

Kurtz discloses wherein said network perimeter comprises entries and exits from said network (see at least, abstract and [0012]).

Claim 10

Kurtz discloses wherein the steps of reviewing security of a network perimeter architecture, reviewing security of data processing devices that transfer data across the perimeter of the network, and reviewing vulnerability of applications or data processing devices within said perimeter from entities outside of said perimeter are performed at least in part with a respective program tool (see at least, abstract, [0012], and [0088]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 3, 11-15, 17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurtz et al. (US 2003/0217039 A1) in view of Chandrashekhar et al. (US 20030212909 A1).

Claim 2

Kurtz fails to disclose further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter.

However Chandrashekhar discloses further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter (see at least, abstract, [0032]: Table 1: Security Layer (Infrastructure) control access and confirm identity and (Application) data is only transmitted between authorized applications and endpoints (e.g. interpreted as inside/outside perimeter (see [0003])).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include further comprising the

step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter as taught by Chandrashekhar. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a systematic way to analyze the security capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, [0003]).

Claim 3

Kurtz fails to disclose further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter.

However Chandrashekhar discloses further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter (see at least, abstract, [0032]: Table 1: Security Layer (Infrastructure) control access and confirm identity and (Application) data is only transmitted between authorized applications and endpoints (e.g. interpreted as inside/outside perimeter (see [0003])).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter as taught by Chandrashekhar. One of ordinary skill in the art would have been motivated

to combine the teachings in order to provide a systematic way to analyze the security capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, [0003]).

Claim 11

Kurtz fails discloses wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter.

However Chandrashekhar discloses wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter (see at least, abstract, [0032]: Table 1: Security Layer (Infrastructure) control access and confirm identity and (Application) data is only transmitted between authorized applications and endpoints (e.g. interpreted as inside/outside perimeter (see [0003])), [0043], [0079]: the examiner notes security assessment tool to identity actual vulnerability, and [0088]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter as taught by Chandrashekhar. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a systematic way to analyze the security

capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, [0003]).

Claim 12

Kurtz fails to disclose wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points.

However Chandrashekhar discloses wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points (see at least, abstract, [0032]: Table 1: Security Layer (Infrastructure) control access and confirm identity and (Application) data is only transmitted between authorized applications and endpoints (e.g. interpreted as inside/outside perimeter (see [0003])), [0043], [0079]: the examiner notes security assessment tool to identity actual vulnerability, and [0088]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points as taught by Chandrashekhar. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a systematic way to analyze the security capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, [0003]).

Claim 13

Kurtz discloses wherein the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises: testing control points with port scans; and testing control points with penetration tests (see at least, [0011]).

Claim 14, 15, 17, and 20

Kurtz discloses the reviewing security of a network perimeter architecture (see at least, abstract and [0012]) the reviewing security of data processing devices that transfer data across the perimeter of the network (see at least, abstract and [0012]).

Kurtz fails to disclose comprising: performing a policy review of an enterprise which owns or controls said network; defining review parameters based upon the policy review; and utilizing the review parameters to perform each of: the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter.

However Chandrashekhar discloses comprising: performing a policy review of an enterprise which owns or controls said network (see at least, [0047]: the examiner notes customer policy); defining review parameters based upon the policy review (see at least, [0047]); and utilizing the review parameters to perform each of: the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from

computers or users outside of said perimeter. (see at least, abstract, [0032]: Table 1: Security Layer (Infrastructure) control access and confirm identity and (Application) data is only transmitted between authorized applications and endpoints (e.g. interpreted as inside/outside perimeter (see [0003])), [0043], [0047], [0079]: the examiner notes security assessment tool to identity actual vulnerability, and [0088]). Further Chandrashekhar discloses [Claim 15] generating, receiving, and performing test cases for each review step (see at least, [0047]: the examiner notes an external test module)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include performing a policy review of an enterprise which owns or controls said network; defining review parameters based upon the policy review; and utilizing the review parameters to perform each of: k, the reviewing security of applications that transfer data across said perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter as taught by Chandrashekhar. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a systematic way to analyze the security capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, [0003]).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892 attached.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571) 270-1385. The examiner can normally be reached on Monday - Friday: 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2439

/Timothy P Callahan/

Director, Technology Center 2400